

ISMAIL J. RAMSEY (CABN 189820)
United States Attorney

THOMAS A. COLTHURST (CABN 99493)
Chief, Criminal Division

CHRIS KALTSAS (NYBN 5460902)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7200
Facsimile: (415) 436-7234
Email: chris.kaltsas2@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

UNITED STATES OF AMERICA,) CASE NO.

Plaintiff,)

v.)

APPROXIMATELY 10 BITCOINS FROM)
DEPOSIT ADDRESSES HELD AT THE OKX)
CRYPTOCURRENCY EXCHANGE,)

Defendant.)

**VERIFIED COMPLAINT FOR CIVIL
FORFEITURE *IN REM***

The United States of America, by its attorneys Ismail J. Ramsey, United States Attorney, and Chris Kaltsas, Assistant United States Attorney for the Northern District of California, brings this complaint and alleges as follows:

NATURE OF THE ACTION

1. This is a judicial forfeiture action *in rem*, as authorized by Title 18, United States Code, Sections 981 and 983.

2. This Court has jurisdiction under Title 18, United States Code, Section 981; and Title 28, United States Code, Sections 1345 and 1355, as the defendant property constitutes or is derived from proceeds obtained, directly or indirectly, from violations of Title 18, United States Code, Sections 1343 and 1956, as well as property involved in violations of Title 18, United States Code, Section 1956.

3. This action is timely filed in accordance with Title 18, United States Code, Section 983.

4. Venue is proper because the defendant property represents the proceeds of a crime that may be prosecuted in the Northern District of California. 28 U.S.C. §§ 1355, 1395.

5. Intra-district venue is proper in the Oakland division within the Northern District of California.

PARTIES

6. Plaintiff is the United States of America.

7. The Defendant Property constitutes 10 Bitcoins (“BTC”) held in deposit addresses located at the OKX cryptocurrency exchange. Those addresses include those ending in LJBC; o2Lc; TA77; hvDx; and sfh8.

BACKGROUND ON CRYPTOCURRENCY

8. Cryptocurrency (also known as virtual or digital currency), a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are BTC, Litecoin, Monero, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers.

9. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “Blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.¹

¹ Some cryptocurrencies, such as Monero, operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

10. BTC is a type of cryptocurrency that allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems. BTC is a decentralized, peer-to-peer form of cryptocurrency having no association with banks or governments. Users can store their bitcoins in digital “wallets,” which are identified by unique electronic “addresses.” A digital wallet essentially stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. To access bitcoins on the public ledger, an individual must use a public address (or “public key”) and a private address (or “private key”). The public address can be analogized to an account number while the private key is like the password to access that account. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger (i.e., the Blockchain), the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as “pseudonymous,” meaning they are partially anonymous. An individual can send and receive Bitcoins through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be performed on any type of computer, including laptop computers and smart phones.

11. The public addresses of Bitcoin wallets are recorded on the Blockchain during transactions involving the Bitcoin wallet. Various software applications are available to both government and private companies which input publicly available data from the Blockchain. These software applications assist with conducting blockchain analysis, which is the process of inspecting, identifying, clustering, modeling and visually representing data with the goal of discovering useful information about the different actors transacting in cryptocurrency. Clustering is the grouping of a set of cryptocurrency wallets in such a way that wallets in the same cluster are associated with and/or controlled by the same individual/entity. Software applications use open source and proprietary data to cluster wallets together. When conducting blockchain analysis, wallet clusters are useful to law enforcement to determine if a specific wallet is being controlled by the same individual or associated with a cryptocurrency exchange or other entity.

12. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of formats, including on a tangible,

1 external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-
2 based cloud storage provider (“online wallet”), as a mobile application on a smartphone or tablet
3 (“mobile wallet”), printed public and private keys (“paper wallet”), and as an online account associated
4 with a cryptocurrency exchange.

5 13. Because desktop, mobile, and online wallets are electronic in nature, they are located on
6 mobile devices (e.g., smartphones or tablets) or at websites that users can access via computer, smart
7 phone, or any device that can search the Internet. Hardware wallets are located on some type of external
8 or removable media device, such as a USB thumb drive or other commercially available device designed
9 to store cryptocurrency (e.g., Trezor, KeepKey, or Nano Ledger). Paper wallets contain an address and a
10 QR code with the public and private key embedded in the code.

11 14. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs,
12 and accessed through a “recovery seed” (random words strung together in a phrase) or a complex
13 password. Additional security safeguards for cryptocurrency wallets can include additional
14 authentication measures such as personal identification numbers (“PINs”) and/or passwords to access
15 the wallet or initiate transactions. Moreover, individuals possessing cryptocurrencies often have
16 safeguards in place to ensure that their cryptocurrencies become further secured in the event that their
17 assets become potentially vulnerable to seizure and/or unauthorized transfer. The Trezor device, for
18 example, offers an advanced passphrase option that incorporates a “25th seed word” that must be
19 enabled to access potentially obscured digital currency assets.

20 15. Some companies offer cryptocurrency wallet services which allow users to download a
21 digital wallet application onto their smart phone or other digital device. A user typically accesses the
22 wallet application by inputting a user-generated PIN or password. Users can store, receive, and transfer
23 cryptocurrencies via the application; however, many of these companies do not store or otherwise have
24 access to their users’ funds or the private keys that are necessary to access users’ wallet applications.
25 Rather, the private keys are stored on the device on which the wallet application is installed (or any
26 digital or physical backup private key that the user creates). As a result, these companies generally
27 cannot assist in seizing or otherwise restraining their users’ cryptocurrency. Nevertheless, law
28 enforcement can seize cryptocurrency from the user’s wallet directly, such as by accessing the user’s

1 smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law
2 enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for
3 a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or
4 reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held
5 within the new wallet to a law-enforcement-controlled wallet.

6 16. According to open-source information, OKX is a Seychelles-based cryptocurrency and
7 derivatives exchange that provides a platform for trading various instruments and cryptocurrency
8 including Bitcoin, Bitcoin Cash, Ethereum, and Litecoin. OKX was previously branded “OKEx,” but
9 changed its name to OKX in January 2022. The OKX platform is not available to U.S. based investors.
10 According to Reuters, in February 2021, OKX saw their biggest trading volume in history at \$188
11 billion.

12 FACTS

13 J.C.’s Involvement with the Initial Scam.

14 17. On June 29, 2022, a resident of San Ramon, California with the initials J.C. contacted the
15 San Ramon Police Department to report having been contacted by individuals claiming to be from
16 various law enforcement agencies. The unidentified individuals convinced J.C. to send approximately
17 \$38,000 worth of Bitcoin to the individuals via various Bitcoin ATMs. A Bitcoin ATM is a device
18 similar to a standard bank ATM. It is generally used to withdraw or transfer funds located in a
19 customer’s Bitcoin wallet.

20 18. According to J.C., they received multiple phone calls from unknown and blocked phone
21 numbers. J.C. answered one of the phone calls and began speaking to an unknown female suspect
22 (hereafter UF1). UF1 claimed to be from the Drug Enforcement Administration (“DEA”), and informed
23 J.C. that the DEA had intercepted a package that was associated with UF1 that contained drugs, and was
24 linked to a physical address in Texas. UF1 further informed J.C. that J.C. could hire lawyers to contest
25 criminal charges that would be brought against J.C., or J.C. could pay money to UF1 to resolve the issue
26 without criminal prosecution. J.C. told UF1 that J.C. would pay money to resolve the matter, and that
27 they lived in San Ramon, CA. UF1 informed J.C. that J.C. would be contacted by J.C.’s local police
28 department.

1 19. J.C. then received a phone call with a phone number that appeared to be attributable to
2 the City of San Ramon, per the caller identification feature on their phone. When J.C. answered the
3 phone, they began speaking with an unidentified male (UM1). J.C. spoke to multiple people around this
4 time and could not recall the order of individuals J.C. spoke with or all of the names claimed by each
5 individual. J.C. recalled at least one male J.C. spoke with claimed to be an officer with the San Ramon
6 Police Department. J.C. also believed at least one person J.C. spoke with had a Middle Eastern accent,
7 and J.C. believes there was speech in the background of the call that sounded like a foreign language.

8 20. J.C. was instructed to withdraw money from J.C.'s bank accounts and to tell the bank that
9 J.C. was taking an overseas vacation if the bank asked questions regarding J.C.'s withdrawals. J.C. went
10 to Patelco Credit Union branches in Walnut Creek, CA and Lafayette, CA and withdrew cash in
11 amounts of \$12,500 and \$25,600, respectively.

12 21. J.C. was instructed to deposit the funds into Bitcoin addresses provided by the unknown
13 individuals on the phone calls. J.C. made five deposits to Bitcoin addresses using various Bitcoin ATM
14 locations in Concord, CA and Walnut Creek, CA in amounts of \$2,950; \$12,050; \$2,900; \$12,100; and
15 \$8,000 (a total of \$38,000) per the unknown individuals' instructions. J.C. made all of these deposits
16 between 4:00PM and 9:00PM on June 29, 2022.

17 22. J.C. was not, in fact, under investigation with the DEA or the San Ramon Police
18 Department. Rather, J.C. fell victim to a law enforcement impersonation scam. These scams rely on the
19 scammers utilizing "spoofed" phone numbers. A "spoofed" phone number is one that appears on a
20 telephone user's caller identification system as attributable to one individual or entity, when in reality,
21 another person or entity is on the line using a different phone number. Spoofing a phone number results
22 in victims of law enforcement impersonation scams receiving phone calls and believing that the
23 individuals calling them are from legitimate law enforcement agencies.

24 23. After spoofing a number and calling a victim, scammers generally attempt to convince
25 the victim that they have committed a crime. The scammers will typically inform the victim that they
26 must pay a certain amount of money to the scammers to avoid arrest and/or prosecution, and these
27 demands are typically for cryptocurrency, including BTC. The nature of cryptocurrency, such as BTC,
28 allows the scammers to move the funds once received from the victim almost instantaneously.

Furthermore, the pseudonymous and decentralized nature of cryptocurrency allows the scammers to move the funds in manners that obfuscate the source of the funds, thwart law enforcement efforts to identify the individual(s) perpetrating these scams, and frustrate efforts of victims to recover their lost funds.

Blockchain Tracing and Identification of the Defendant Property.

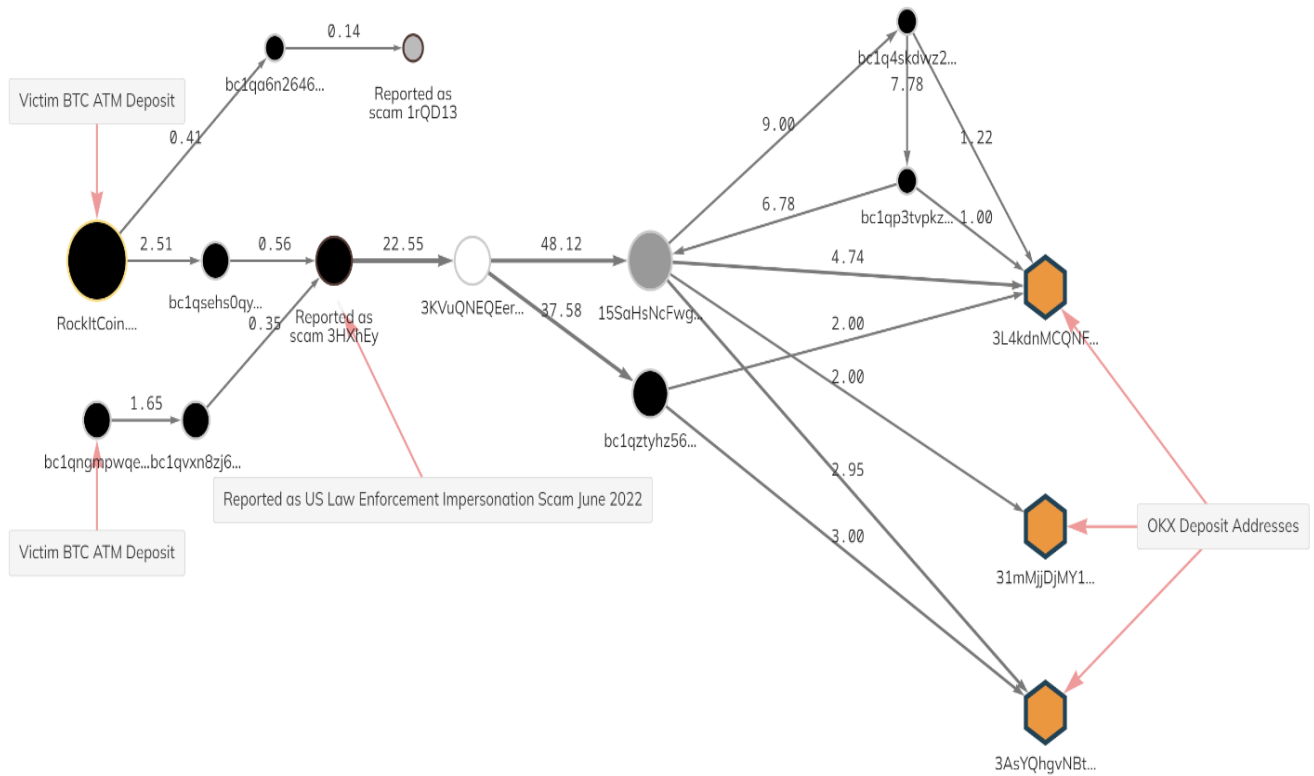
24. Based on the information provided by J.C., law enforcement began tracing the transfers of BTC from the BTC wallets. That tracing began with the addresses to which J.C. sent the aforementioned BTC, which include the following addresses:

- 1rQD13a4PUde63T6rhHEGvSGm5qHfuz5N
- 3LeWNF8a9f2HWGiZHLVEJu1Ch8VEAjwGge
- 33UXNxntLJVj9MW9crl2qzk5St9ragfrG

25. Blockchain analysis revealed that the BTC sent to two of the addresses to which J.C. had sent the majority of the funds, 0.90954981 BTC, were consolidated together into another address that had received a total of 13.76109241 BTC deposits at the time the government's tracing analysis was conducted. The fraudulently obtained BTC was then deposited into addresses believed to be under the control of cryptocurrency exchanges, including OKX. In six of those transactions, a total of 10.69 BTC was deposited into the following three addresses held at OKX (hereafter the "OKX INITIAL ADDRESSES"), to wit:

- 3L4kdnMCQNFBEYpCdYnYnSeeTcU2C2HnVd
- 31mMjjDjMY1ULDU7WAXvgt1pRxeuWkCjeC
- 3AsYQhgvNBtwa67z59KU3gsmJNhDp7XHDW

The chart below depicts the flow of funds from J.C.'s deposits in the Bitcoin ATMs, consolidation of J.C.'s funds with other funds, and transfers to the OKX INITIAL ADDRESSES.



26. As the chart indicates, J.C.'s funds went through a number of transfers before being transferred to the OKX INITIAL ADDRESSES. Criminals will often conduct an otherwise unnecessary number of transactions in the transfer of funds (or "hops") in an effort to layer ill-gotten funds and disguise the illicit source. "Layering" is the process through which money launderers attempt to combine the proceeds of fraud with funds otherwise untraceable to criminal activity in an attempt to hide the nature, source, ownership, or control of proceeds of fraud. Moreover, the number of hops in this transaction strongly indicates that the movement of funds was performed in a manner meant to conceal the nature, source, control, and/or ownership of the proceeds of a specified unlawful activity, to wit, wire fraud.

27. Individuals involved in scams, including law enforcement impersonation scams, will frequently comingle funds from numerous victims into individual accounts or cryptocurrency wallets. They will also frequently move the proceeds of scams through numerous cryptocurrency wallets and comingle the scam proceeds with other funds, including funds from non-illicit sources. They also rapidly

1 transfer funds to obfuscate the source of the illicit funds and attempt to make the illicit funds appear to
2 be legitimate funds.

3 28. The initial investigation revealed that, at the time that no funds remained in the customer
4 accounts linked to the OKX INITIAL ADDRESSES. Moreover, the customer accounts linked to the
5 OKX INITIAL ADDRESSES were opened using minimal user-provided information and deposits into
6 the accounts were kept just below the OKX threshold that would require additional customer due
7 diligence on the part of OKX, another indication that the OKX accounts were used in furtherance of
8 money laundering. The customer accounts were used for a week at a time and then abandoned in favor
9 of new accounts.

10 29. The investigation revealed five additional addresses associated with OKX customer
11 accounts that were likely controlled by the same person or persons who controlled the OKX INITIAL
12 ADDRESSES. All eight OKX wallet addresses (the OKX INITIAL ADDRESSES and the five
13 additional wallet addresses) were linked together either by device(s) used to access the accounts, IP
14 addresses, or withdrawal addresses. Each of the additional addresses held a balance of exactly 2 BTC,
15 for a total of 10 BTC. Those additional addresses were the five aforementioned BTC addresses, and the
16 BTC seized from those addresses constitute the Defendant Property. Those BTC addresses all end with
17 the following numbers and letters:

- 18 • LJBC;
- 19 • o2Lc;
- 20 • TA77;
- 21 • hvDx; and
- 22 • sfh8.

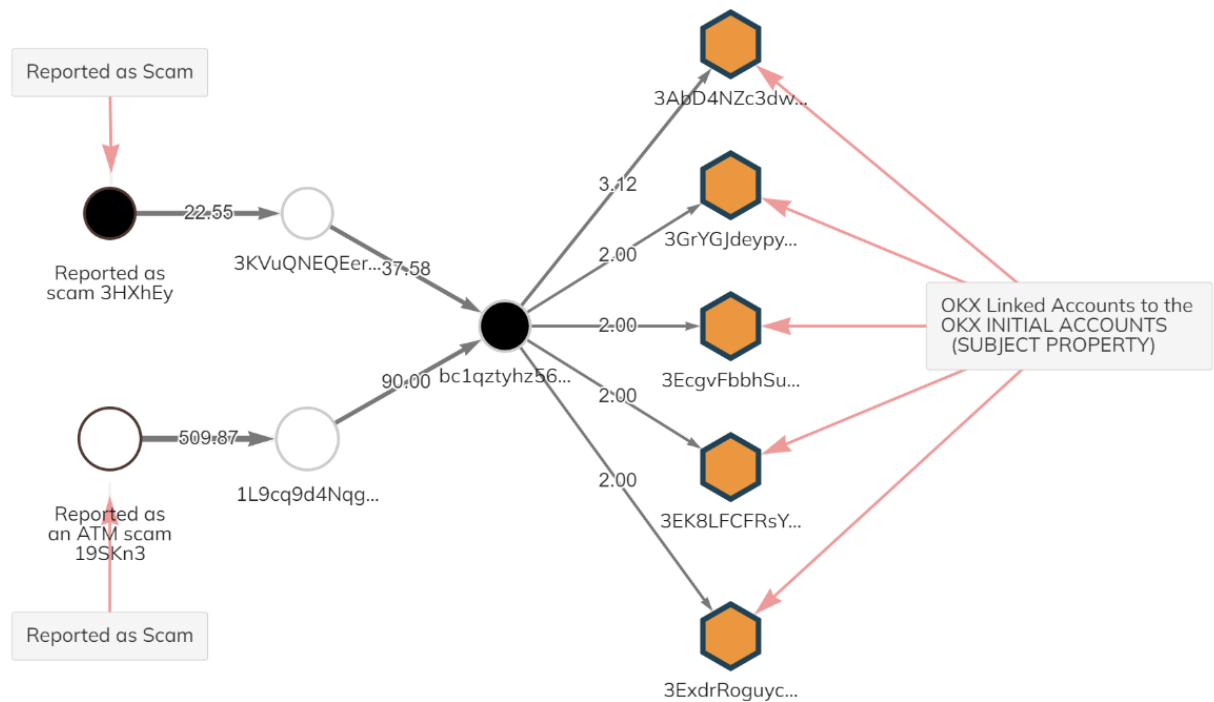
23 30. Based on blockchain analysis, each of the addresses above was active for no longer than
24 5 days during the period from July 15, 2022 through July 20, 2022. Sources of funds deposited into the
25 addresses containing the Defendant Property were traceable to BTC wallet clusters identified with
26 Bitcoin ATMs, cryptocurrency exchanges, and clusters reported as scams. These reported scams include
27 at least four separate complaints filed with the Internet Crime Complaint Center (“IC3”) between May
28 24, 2022 and August 8, 2022. These complaints all concerned law enforcement impersonation scams

similar to the one reported by J.C., including reports from individuals contacted by scammers claiming to be U.S. Marshals and/or Customs and Border Protection Officers. In each of these complaints, the complainants indicated that the scammer instructed the victims to send cryptocurrency to wallet clusters as a result of criminal violations the scammer alleged the victim to have committed.

31. In summary, on June 29, 2022, J.C. was instructed to deposit approximately \$38,000 in various Bitcoin ATMs by unknown individuals claiming to be law enforcement officers from the DEA and San Ramon Police Department. After making the deposits, the BTC was transferred to various wallets, comingled with additional funds (including funds from wallet clusters associated with law enforcement impersonation scams) and transferred to wallets including the OKX INITIAL ADDRESSES. The investigation identified 5 additional wallet addresses containing the Defendant Property associated to the OKX INITIAL ADDRESSES by technical and transaction characteristics. The five wallet addresses constituting the Defendant Property all received BTC from one wallet address, which itself received funds associated with clusters reported as scams.

32. On July 20, 2022, all five addresses that make up the SUBJECT PROPERTY each received a transfer of BTC from a cluster of addresses identified by the root address bc1qztyhz5696l3xftp0ja725j5snuwy2v0srvrhgr (hereafter the bc1qz cluster). The “root address” of a cluster is the first address in the cluster to appear on the blockchain. Between July 12, 2022 and July 26, 2022, the bc1qz cluster received 8 Bitcoin transfers totaling approximately 37.58 BTC from another cluster identified by the root address 3KVuQNEQEer8jJRu3tg6AdU98HESv2UByD (hereafter the 3KVuQ cluster). Additionally, the bc1qz cluster received exactly 90 BTC from a cluster of addresses identified by the root cluster 1L9cq9d4NqgEGSc1DNCWtct4yRQo1vE9tT (hereafter the 1L9cq cluster) in 8 separate transactions between July 8, 2022 and July 19, 2022. The 3KVuQ cluster received approximately 22.55 BTC and the 1L9cq cluster received approximately 509.87 BTC between March 2022 and July 2022 directly from wallet clusters that have been reported as scams. The chart below shows the movement of funds from wallet clusters reported as scams to the SUBJECT PROPERTY. Both of wallet clusters are associated with reports from victims of scams involving cryptocurrency ATMs.

//



33. Individuals involved in scams, including law enforcement impersonation scams, will frequently conduct voluminous and complex transactions to move the illicit funds gained from the scams. These movements typically involve the use of various cryptocurrency exchanges and other cryptocurrency wallets in an attempt to break the chain from the source of the funds and attempt to conceal the original nature of the funds.

34. Moreover, individuals utilizing cryptocurrency exchanges to convert the proceeds of funds from cryptocurrency to fiat currency (such as U.S. Dollars, Euros, etc.) will frequently establish multiple accounts and vary the accounts used to receive and transact with any accounts containing illicit funds. Individuals involved in scams will frequently avoid conducting transactions above individual cryptocurrency exchange company thresholds in order to avoid inquiries from the exchange and scrutiny of their account(s). Conducting transactions above these thresholds may engender enhanced paperwork requirements, additional identity verifications, and other processes that could reveal the true identity of the individual engaging in these illicit transactions.

35. The evidence indicates that the Defendant Property was controlled by the same person or persons who were in control of the OKX INITIAL ACCOUNTS that received illicit funds, including funds originating from J.C. and/or funds comingled with funds originating from J.C. in an attempt to conceal the source, nature, location, or ownership of the funds. Furthermore, the evidence indicates that the SUBJECT PROPERTY has received funds, including comingled funds, from wallets that have been reported as scams.

COUNT ONE

Civil Forfeiture (Title 18, United States Code, Section 981(a)(1)(C)) for Wire Fraud (Title 18, United States Code, Section 1343)

36. Civil forfeiture of the proceeds of wire fraud is authorized by Title 18, United States Code, Section 981(a)(1)(C). Specifically, Section 981(a)(1)(C) authorizes forfeiture of “any property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting ‘specified unlawful activity’ (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense.” Section 1956(c)(7)(A) defines the term “specified unlawful activity” as including “any act or activity constituting an offense listed in section 1961(1) of this title.” And Title 18, United States Code, Section 1961(1), in turn, includes violations of Title 18, United States Code, Section 1343 in its definition of racketeering activity.

37. The Defendant Property constitutes, and is derived from, the proceeds of wire fraud, and is thus subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C).

COUNT TWO

Civil Forfeiture (Title 18, United States Code, Section 981(a)(1)(A)) for Money Laundering (Title 18, United States Code, Section 1956(a)(1)(B)(i))

38. Civil forfeiture of property involved in a money laundering transaction, or property traceable to such property, is authorized by Title 18, United States Code, Section 981(a)(1)(A), which allows the United States to forfeit “any property, real or personal, involved in a transaction . . . in violation of section 1956 . . . of this title, or any property traceable to such property.”

39. A violation of Title 18, United States Code, Section 1956(a)(1)(B)(i) occurs when a person conducts or attempts to conduct a financial transaction knowing that the transaction involves the

1 proceeds of a specified unlawful activity when the transaction is designed in whole or part “to conceal or
2 disguise the nature, the location, the source, the ownership or the control of the proceeds of the specified
3 unlawful activity; or . . . to avoid a transaction reporting requirement under State or Federal law”, or
4 involves property “traceable to such property.”

5 40. Wire fraud is a specified unlawful activity pursuant to Title 18, United States Code,
6 Sections 1956(c)(7)(A) and 1961(1). Thus, the Defendant Property is subject to forfeiture pursuant to
7 Title 18, United States Code, Section 981(a)(1)(A) because it was involved in, or is traceable to property
8 involved in, money laundering transactions in violation of Title 18, United States Code, Section
9 1956(a)(1)(B)(i).

10 **PRAYER FOR RELIEF**

11 41. The United States requests that due process issue to enforce the forfeiture of the above
12 listed Defendant Property; that notice be given to all interested parties to appear and show cause why
13 forfeiture should not be decreed; that the Court enter a judgment forfeiting the Defendant Property; and
14 that the United States be awarded such other relief as may be proper and just.

15
16 DATED: June 29, 2023

Respectfully submitted,

17 ISMAIL J. RAMSEY
18 United States Attorney

19 /S/
20 CHRIS KALTSAS
21 Assistant United States Attorney
22
23
24
25
26
27
28

VERIFICATION

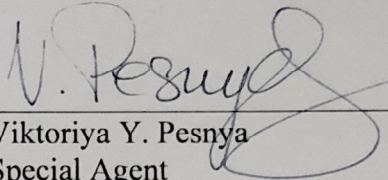
I, Viktoriya Y. Pesnya, state as follows:

1. I am a Special Agent with the Internal Revenue Service-Criminal Investigation. I am one of the agents working on this case. As such, I am familiar with the facts and the investigation leading to the filing of this Complaint for Forfeiture.

2. I have read the Complaint and affirm that the allegations contained therein are true.

* * *

I declare under penalty of perjury that the foregoing is true and correct. Executed this 28 day of June, 2023 in Hayward, California.


Viktoriya Y. Pesnya
Special Agent
Internal Revenue Service-Criminal Investigation